UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

DEBORAH JO BAILEY,

Plaintiff,

v.

Case No. 07-11672
Hon. Sean F. Cox

JEFFERY ALLAN BAILEY, et al.,

Defendants.

---

**OPINION AND ORDER**

This matter is before the Court on Defendant Jeffrey Bailey's Motion for summary judgment; and Defendant Todd Pope's Motion for summary judgment. All parties have briefed the issues and a hearing was held January 17, 2008. For the following reasons, the Court **GRANTS** Defendant Todd Pope's Motion for summary judgment; and **GRANTS** in part, and **DENIES** in part, Defendant Jeffrey Bailey's Motion for summary judgment. Summary judgment is granted on Plaintiff's claims for: (1) violation of 18 U.S.C. § 2511; (2) violation of 18 U.S.C. § 2512; (3) MCL § 750.539a, et seq.; (4) MCL § 750.540; (5) invasion of privacy against Defendant Pope based on intrusion upon seclusion; (6) invasion of privacy based on public disclosure; and (7) intentional infliction of emotional distress. Summary judgment is denied on Plaintiff's claims for: (1) violation of 18 U.S.C. § 2701 against Defendant Bailey; and (2) invasion of privacy against Defendant Bailey based on intrusion upon seclusion. Additionally, Defendant Andrew Kozyra is **DISMISSED** from this action.

## I. BACKGROUND

This case arises out of Defendant Jeffrey Bailey's installation of a key logger on a computer shared by him and his now ex-wife, Plaintiff Deborah Jo Bailey.

Plaintiff and Defendant Bailey were married in 1987 and had three children. Unfortunately, the marriage began to deteriorate. Defendant Bailey had suspicions about Plaintiff's use of the internet, which he believed was excessive. According to Defendant Bailey, in fall of 2005 he clicked onto his wife's email account, titled joy2u. He saw several alerts that there were messages for Plaintiff from a website called Killer Movies Forum. Defendant Bailey clicked on the hyperlink associated with the alerts and read the messages. The messages were from a person known as "Finti" and were of a sexual nature. Plaintiff admitted to sexual discussions with Finti and others, but denies her children were aware of the discussions.

Shortly after Defendant Bailey discovered Plaintiff's sexual discussions, she opened a new email account titled chloedebb@yahoo.com. Around the same time, Defendant Bailey downloaded a free trial version of a key logger software and installed it on both home computers. The program is designed to record every keystroke made on the computer and store it in a text file on the computer's hard drive. The parties dispute whether the file storing the keystroke information can be accessed only on the computer where the software is installed, or whether it can be accessed remotely. Defendant Bailey used the key logger program to learn the password for both Plaintiff's chloedebb@yahoo.com email account and her private messaging system on the Killer Movies Forum. Defendant Bailey learned that Plaintiff was continuing her internet sexual activities.

On January 9, 2006, Defendant Bailey left the marital home with the three children and

went to Ohio to stay with his brother. In anticipation of divorce proceedings, Defendant Bailey provided his attorney, Defendant Todd Pope, with copies of emails and messages taken from the home computer. Throughout the divorce proceedings, Defendant Bailey supplied Defendant Pope with copies of emails and messages he said he was able to access because he had Plaintiff's passwords, by virtue of the key logger program. However, Defendant Bailey denies that he accessed the key logger program on the home computer after he left on January 9, 2006. Instead, he claims he continued to access Plaintiff's accounts using the passwords he had obtained using the key logger, or by guessing her new passwords which he claims all used family names. Plaintiff also had her daughter Chloe set up another email account titled debbiejo_crazy@yahoo.com. Chloe gave the password to Defendant Bailey.

Defendant Bailey filed for divorce on January 11, 2006. He alleged Plaintiff was an alcoholic with a history of depression and sought full physical custody of the children. Defendant Bailey was granted temporary custody. Plaintiff hired an attorney, Defendant Andrew Kozyra. The custody order was amended to grant Plaintiff parenting time every third weekend, with the condition that neither party was allowed to consume alcohol during their parenting time. During further custody proceedings, Plaintiff testified that she had not consumed alcohol recently and was voluntarily undergoing alcohol and drug testing. Defendant Pope impeached her testimony using emails provided to him by Defendant Bailey. The emails indicated that Plaintiff had recently gone to a party where she consumed alcohol and illegal drugs.

On May 18, 2006, Defendant Pope sent a request to admit the genuineness of the email and message copies provided by Defendant Bailey, to Defendant Kozyra. Defendant Kozyra, on behalf of Plaintiff, moved for a protective order. His request was denied.

On July 16, 2006, Plaintiff was cited for a second drinking offense. The parties settled the divorce case prior to the July 21, 2006 trial date. Plaintiff agreed to give full physical custody of the children to Defendant Bailey. Plaintiff was to receive parenting time, including two non-consecutive weeks in the summer. The judgment of divorce was entered on August 31, 2006. Within two weeks of entry of the judgment, Plaintiff was again arrested for driving while intoxicated. Defendant Bailey moved to suspend Plaintiff's parenting time. At the hearing, the judge indicated he was very concerned about Plaintiff's sobriety. A hearing was held on January 5, 2007 on Defendant Bailey's motion to suspend parenting time. At the hearing, the judge heard testimony that Plaintiff made allegations of sexual assault against Defendant Bailey regarding their daughter Chloe. He also heard testimony from a neighbor that during a visit in August, Plaintiff was "highly intoxicated" and the neighbor took care of the children while Defendant Bailey drove from Ohio to pick them up. The parties' daughter Chloe also testified that she had witnessed her mother intoxicated during the visit. The judge concluded Plaintiff was harming her children and suspended her parenting time. After this hearing, Plaintiff was arrested for domestic violence against Defendant Bailey and found in contempt of court for emailing her children. At a March 2, 2007 hearing, the judge awarded sole legal and physical custody to Defendant Bailey. Plaintiff has only recently been given parenting time in the form of supervised visitation one weekend per month at her father's home.

Plaintiff argues that she would not have lost custody of her children if her emails and internet messages had not been disclosed. She also attributes emotional problems and distress she claims to suffer to the loss of custody of her children.

On April 13, 2007, Plaintiff filed the instant action. On August 28, 2007, an Amended

Complaint was filed alleging: (1) violation of 18 U.S.C. § 2511 against Defendants Bailey and Pope; (2) violation of 18 U.S.C. § 2701 against Defendant Bailey; (3) violation of 18 U.S.C. § 2512 against Defendants Bailey and Pope, and against a John Doe Defendant who supplied the key logger software; (4) violations of MCL § 750.539a, et seq., and MCL § 750.540 against Defendants Bailey, Pope and John Doe; (5) invasion of privacy against Defendants Bailey and Pope; (6) intentional infliction of emotional distress against all Defendants; and (7) professional malpractice against Defendant Kozyra. Also on April 13, 2007, Plaintiff filed a motion for preliminary injunction to prevent further use of the key logger software, the parties entered a stipulation following a status conference.

On October 22, 2007, Defendants Bailey and Pope filed separate Motions for summary judgment as to all claims.

## II. STANDARD OF REVIEW

Under Fed. R. Civ. P 56(c), summary judgment may be granted "if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." *Copeland v. Machulis*, 57 F.3d 476, 478 (6th Cir. 1995). A fact is "material" and precludes a grant of summary judgment if "proof of that fact would have [the] effect of establishing or refuting one of the essential elements of the cause of action or defense asserted by the parties, and would necessarily affect application of appropriate principle[s] of law to the rights and obligations of the parties." *Kendall v. Hoover Co.*, 751 F.2d 171, 174 (6th Cir. 1984). The court must view the evidence in the light most favorable to the nonmoving party and it must also draw all reasonable inferences in the nonmoving party's favor.

*Cox v. Kentucky Dept. of Transp*., 53 F.3d 146, 150 (6th Cir. 1995).

## III. ANALYSIS

### A. 18 U.S.C. § 2511 - The Wiretap Act

Plaintiff alleges Defendants Pope and Bailey violated 18 U.S.C. § 2511 when they obtained Plaintiff's emails and messages using the passwords learned from the key logger. Section 2511 provides, in pertinent part:

> (1) Except as otherwise specifically provided in this chapter any person who -
>
> > (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
> > * * *
> >
> > (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
> > (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection...
>
> shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

The parties dispute whether Defendants' conduct is actionable under the Wiretap Act because, according to Defendants, there was no "interception" as that term has been interpreted by the courts. Specifically, the parties disagree on whether "interception" requires that the electronic communication be intercepted contemporaneously with its transmission. There is no Sixth Circuit authority on the issue.

Although the issue has not been addressed by the Sixth Circuit, the Circuits that have

addressed the issue have agreed that the definition of "intercept" "encompasses only acquisitions contemporaneous with transmission." *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003). See *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994); *Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868 (9th Cir. 2001); *In re Pharmatrak, Inc*., 329 F.3d 9 (1st Cir. 2003); and *Fraser v. Nationwide Mutual Ins. Co.,* 352 F.3d 107 (3rd Cir. 2003). The general reasoning behind these decisions is that based on the statutory definition and distinction between "wire communication" and "electronic communication," the latter of which conspicuously does not include electronic storage, Congress intended for electronic communication in storage to be handled solely by the Stored Communications Act. This interpretation is reasonable and consistent with the language of the statute.

Plaintiff does not offer argument or authority that contradicts the reasoning offered by the cases cited above. Instead, Plaintiff directs this Court to the "leading case" of *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005). Plaintiff claims that the *Councilman* court "determined that the contemporaneous requirement which had been inserted by earlier courts, was not a requirement under a proper interpretation of the Electronic Communications Privacy Act..." [Response, p.4]. Plaintiff mischaracterizes the *Councilman* case. First, the *Councilman* court did not address the issue of whether the contemporaneous requirement applied: "this appeal does not implicate the question of whether the term 'intercept' applies only to acquisitions that occur contemporaneously with the transmission of a message from sender to recipient..." *Id.* at 80. What the *Councilman* court ruled was that the term "electronic communication" as used in the Wiretap Act includes "the transient electronic storage that is intrinsic to the communication process for such communications." *Id.* at 79. In *Councilman*, the defendant argued that because

the original transmission of an email over the internet involves several minuscule stops at other computers, the Wiretap Act did not apply because it did not encompass electronic communications that were in electronic storage no matter how brief the storage. The *Councilman* court, after an exhaustive analysis, did not agree.

This case is more analogous to *Steiger, supra*. In *Steiger*, an anonymous source hacked into the defendant's computer by using a "Trojan Horse" virus. Once the virus was downloaded, the anonymous source was able to access and download information stored on the defendant's computer. The anonymous source found evidence of child sexual abuse and turned the defendant over to the proper authorities. The virus used in *Steiger* only allowed the source to access the defendant's files, it did not "intercept" them while in transit. Similar to the *Steiger* case, here, the key logger only allowed Defendant Bailey to learn passwords, which were used to access and copy Plaintiff's email and messages. Defendant Bailey did not obtain the emails or messages contemporaneously with their transmission, and thus, the Wiretap Act does not apply.

Defendants are entitled to summary judgment on Plaintiff's claim for violation of 18 U.S.C. § 2511.

**B. 18 U.S.C. § 2701 - Stored Communications Act**

Plaintiff alleges Defendant Bailey violated 18 U.S.C. § 2701 when he accessed her emails and messages. Section 2701 provides, in pertinent part:

(a) **Offense** - Except as provided in subsection (c) of this section whoever -

> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> (2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic

> communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

"Electronic storage is defined as either "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

Defendant Bailey argues that the Stored Communications Act does not apply because the emails and messages he accessed were already opened by Plaintiff. Defendant Bailey conflates the two meanings of "electronic storage" and states that "electronic storage" "renders only those stored communications which are temporarily stored or stored for purposes of backup protection incidental to the electronic transmission thereof." [Motion, p.18]. From this Defendant Bailey concludes that once the electronic communication is transmitted to its intended recipient, the Stored Communications Act no longer applies. Defendant Bailey does not cite any significant authority to support his interpretation. He directs the Court to *Bansal v. Russ*, 513 F.Supp.2d 264, 276 (E.D.Pa. 2007), where the Pennsylvania district court, without providing any analysis or citation to authority, found that "[t]he Stored Communications Act...does not prohibit...obtaining 'opened' emails." Defendant Bailey also relies on *Fraser*, 352 F.3d 107, for the proposition that emails that were accessed were not in temporary storage, or backup storage, but were in post transmission storage. However, what the *Fraser* court actually held was:

> Rather, according to the District Court, the e-mail was in a state it described as 'post-transmission storage.' We agree that Fraser's e-mail was not in temporary, intermediate storage. But to us it seems questionable that the transmissions were not in backup storage - a term that neither the statute nor the legislative history defines. Therefore, while we affirm the District Court, we do so through a different analytical path, assuming without deciding that the e-mail in question

was in backup storage.

*Id.* at 114. Thus, the *Fraser* case is of no value on this issue.

The Sixth Circuit has not ruled on this issue. However, Defendant's argument was considered by the Ninth Circuit in *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2003). *Theofel* stems from commercial litigation. The defendant sought access to the plaintiff's email and served an obviously over broad subpoena on the plaintiff's internet service provider ("ISP"). Due to the large number of documents encompassed by the subpoena, the ISP provided a sample containing 339 emails. Included in the sample were emails that did not pertain to the matter at hand, and that contained personal or privileged information. Several of the individuals affected brought suit against the defendant alleging violation of the Stored Communications Act. The district court dismissed the plaintiffs' case finding that the access was authorized due to the subpoena. The circuit court disagreed, because the scope of the subpoena was so overly broad the defendant's knew they were not entitled to access all of the documents requested. Similar to Defendant Bailey's argument, the defendant made the alternative argument that emails remaining on the ISP's server after delivery do not fall within the Stored Communications Act's coverage. The court disagreed. The court held that those messages were not within the purview of the subsection (A) definition, but fit comfortably in subsection (B). The court stated:

> There is no dispute that messages remaining on NetGate's server after delivery are stored 'by an electronic communication service' within the meaning of 18 U.S.C. § 2510(17)(B). The only issue, then, is whether the messages are stored 'for purposes of backup protection.' 18 U.S.C. § 2510(17)(B). We think that, within the ordinary meaning of those terms, they are.
>
> An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again -if, for example, the message is accidentally erased from the

> user's own computer. The ISP copy of the message functions as a 'backup' for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition.

*Theofel*, 359 F.3d at 1075 (internal citations omitted).

This court agrees with the reasoning in *Theofel*. The fact that Plaintiff may have already read the emails and messages copied by Defendant does not take them out of the purview of the Stored Communications Act. The plain language of the statute seems to include emails received by the intended recipient where they remain stored by an electronic communication service. The phrase "such communication" in § 2510(17)(B) refers to "wire or electronic communications" as mentioned in (17)(A) - it does not also include the requirement that the electronic communications be "incidental to the electronic transmission thereof." If that were the case, there would be no need to write them as two separate meanings. However, as a point of clarification, Stored Communications Act protection does not extend to emails and messages stored only on Plaintiff's personal computer. *In re Doubleclick Inc*., 154 F.Supp.2d 497, 511 (S.D.N.Y. 2001)("the cookies' residence on plaintiffs' computers does not fall into § 2510(17)(B) because plaintiffs are not 'electronic communication service' providers."). Defendant does not set forth any other basis for dismissing the claim. Accordingly, Defendant Bailey is not entitled to summary judgment on Plaintiff's claim for violation of 18 U.S.C. § 2701.

**C. 18 U.S.C. § 2512 - Wiretap Act**

Plaintiff alleges violation of 18 U.S.C. § 2512 against Defendants Bailey, Pope and a John Doe, the manufacturer of the key logger software. However, there is no private right of action under § 2512. 18 U.S.C. § 2520 provides:

> (a) In general. - Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

Based on the clear language of the statute, a civil cause of action arises only when violation of the statute results in a person's wire, oral, or electronic communication being intercepted, disclosed, or intentionally used. Here, Plaintiffs allegation of violation of § 2512 does not satisfy the requirements of § 2520. Section 2512 deals with the manufacture, sale and possession of particular devices. Violation of the statute has nothing to do with the actual interception, disclosure or use of Plaintiff's electronic communication. See *DIRECTV, Inc. v. Treworgy*, 373 F.3d 1124 (11th Cir. 2004).

Accordingly, Defendants are entitled to summary judgment on Plaintiff's claim for violation of 18 U.S.C. § 2512.

**D. MCL § 750.539a, et seq. - Eavesdropping Statutes**

Plaintiff alleges various violations of Michigan's eavesdropping statutes against Defendants Bailey and Pope.

Defendant Bailey argues the Michigan statutes do not apply because the key logger software is not a "device" as contemplated by the eavesdropping statutes. Defendant Pope argues the Michigan eavesdropping statutes do not apply because Defendant Bailey did not "eavesdrop" on a "private conversation." Plaintiff, without citation to authority, states that the federal Wiretap Act definition of device is analogous to the definition intended by the Michigan eavesdropping statutes, and thus the key logger is a device. Plaintiff does not respond to Defendant Pope's arguments.

A plain reading of the eavesdropping statutes indicates that they do not apply to the circumstances of this case. MCL § 750.539c provides:

> Any person who is present or who is not present during a private conversation and who wilfully uses any device to eavesdrop upon the conversation without the consent of all parties thereto, or who knowingly aids, employs or procures another person to do the same in violation of this section, is guilty of a felony punishable by imprisonment in a state prison for not more than 2 years or by a fine of not more than $2,000.00, or both.

MCL § 750.539d provides, in pertinent part:

> (1) Except as otherwise provided in this section, a person shall not do either of the following:
>
> > (a) Install, place, or use in any private place, without the consent of the person or persons entitled to privacy in that place, any device for observing, recording, transmitting, photographing, or eavesdropping upon the sounds or events in that place.
> > (b) Distribute, disseminate, or transmit for access by any other person a recording, photograph, or visual image the person knows or has reason to know was obtained in violation of this section.
>
> * * *

With respect to § 750.539c, the device must be used with respect to a "conversation." The key logger software only stores as a text file the keys that are pressed on the keyboard of the computer on which the software is installed. When Plaintiff pressed the keys to enter her passwords, compose messages, or compose emails, she was not engaging in a conversation. First, she was not in a direct dialogue with anyone else. Second, the device, the key logger, only recorded her keystrokes, not the response of the other side. The Merriam-Webster Dictionary defines "conversation" as "(1) oral exchange of sentiments, observations, opinions, or ideas; (2) an instance of such exchange." MERRIAM-WEBSTER ONLINE DICTIONARY. The "device" does not record an exchange, but only records keystrokes. This statute was meant to prohibit

eavesdropping in the traditional sense of recording or secretly listening to audible conversation. This is bolstered by the fact that the Michigan legislature felt the need to add a statute that deals specifically with the reading or copying of any message from a computer without authorization. MCL § 750.540. Section 750.540 would be redundant if § 750.539c already prohibited the same. Accordingly, Defendants are entitled to summary judgment on Plaintiff's claim of violation of MCL § 750.539c.

With respect to MCL § 750.539d, the device must observe, record, transmit, photograph, or eavesdrop "upon the sounds or events in that place." This description does not encompass a key logger which only records electronically what keystrokes are pressed on a keyboard. It does not record sounds or events. Further, as discussed above, if that were the contemplated scope of § 750.539d, there would have been no need for § 750.540. Defendants are entitled to summary judgment on Plaintiff's claim for violation of MCL § 750.539d.

Plaintiff also alleges violations for MCL §§ 750.539e and 750.539j. Defendants are entitled to summary judgment on Plaintiff's claim for violation of § 750.539e because it is dependent on the use of information obtained in violation of the eavesdropping statutes, which Defendants are found not to have violated. Defendants are entitled to summary judgment on Plaintiff's claim for violation of § 750.539j because a civil action does not arise from violation of that statute. MCL § 750.539h provides that civil remedies are available only to parties to a conversation upon which eavesdropping is practiced, which is not the substance of a § 750.539j violation.

**E. MCL § 750.540**

Plaintiff alleges a violation of MCL § 750.540 against Defendants Bailey and Pope.

Section 750.540 prohibits the reading or copying of messages sent via a computer without authorization. However, violation of MCL § 750.540 does not appear to give rise to civil liability. The language of § 750.540 only addresses criminal sanctions, it does not mention civil penalties. Moreover, the only statute in the chapter that discusses civil liability is MCL § 750.539h, which states '[a]ny parties to any conversation upon which eavesdropping is practiced contrary to this act shall be entitled to the following civil remedies." As discussed above, Plaintiff's allegations do not amount to eavesdropping of a conversation as contemplated by the eavesdropping statutes. Thus, § 750.539h does not serve to supply a civil cause of action for violation of § 750.540.

"The general rule of law in Michigan is that, where a new right is created or a new duty is imposed by a statute, the remedy provided by the statute for enforcement of the right or for nonperformance of the duty is exclusive unless the remedy is plainly inadequate." *Forster v. Delton School District*, 176 Mich.App. 582, 584 (Mich.App. 1989). "Therefore a private cause of action must be dismissed under a statute creating a new right or imposing a new duty unless the private cause of action was expressly created by the act or inferred from the fact that the act provides no adequate means of enforcement of its provisions." *Id.* at 585. Here, § 750.540 does not expressly provide for a private cause of action, and does provide for adequate enforcement by creating criminal penalties. See *Central Bank of Denver v. First Interstate Bank of Denver*, 511 U.S. 164, 190 (1994)("[W]e refuse[] to infer a private right of action from 'a bare criminal statute'... [a]nd we have not suggested that a private right of action exists for all injuries caused by violations of criminal prohibitions."). Accordingly, Defendants are entitled to summary judgment on Plaintiff's claim for violation of § 750.540.

### F. Invasion of Privacy

Plaintiff alleges a claim for invasion of privacy against Defendants Bailey and Pope. The tort of invasion of privacy has four distinct theories, in this case, Plaintiff alleges two theories: (1) the intrusion upon another's seclusion; and (2) a public disclosure of private facts about the individual. *Lewis v. LeGrow*, 258 Mich.App. 175, 193 (Mich.App. 2003).

#### 1. Intrusion upon seclusion

"There are three necessary elements to establish a prima facie case of intrusion upon seclusion: (1) the existence of a secret and private subject matter; (2) a right possessed by the plaintiff to keep that subject matter private; and (3) the obtaining of information about that subject matter through some method objectionable to a reasonable man." *Id.* "An action for intrusion upon seclusion focuses on the manner in which the information was obtained, not on the information's publication." *Id.*

As an initial matter, this cause of action cannot be maintained against Defendant Pope because there is no evidence that he participated in the "intrusion." The fact that Pope was aware of how Defendant Bailey obtained the emails and messages is irrelevant. See *Doe v. Mills*, 212 Mich.App. 73, 89-91 (Mich.App. 1995). Defendant Pope is entitled to summary judgment on this claim.

With respect to Defendant Bailey, he argues that Plaintiff cannot establish a claim because his actions are not objectionable to a reasonable man. Defendant Bailey contends that his actions were done after inadvertently discovering his wife was having sexual discussions on the internet, and were done to protect himself and his family. Plaintiff responds by stating there is a question of fact, but does not identify any authority or evidence to support his conclusion.

The facts are largely undisputed in this case. The method used by Defendant Bailey was a key logger that recorded Plaintiff's keystrokes, which Defendant used to learn Plaintiff's passwords. With the passwords, Defendant was able to access Plaintiff's email and private message forums. In addition, once Defendant learned that Plaintiff used family names as passwords, he claims he was able to guess her new passwords even after she repeatedly changed them. Plaintiff avers that Defendant continued to access her email even after divorce proceedings were complete. [Plaintiff's Exhibit A]. She provides an affidavit that claims she planted a false story of an affair with a neighbor in an email on January 2007, well after the divorce was final. She claims that on February 16, 2007, her daughter Chloe sent an email referencing the planted story, which Plaintiff takes to mean Defendant Bailey was continuing to access her accounts and passing the information to their teenage daughter.

Defendant cites *Lewis v. Dayton-Hudson*, 128 Mich.App. 165 (Mich.App. 1983), to support his contention that he is entitled to summary judgment. Defendant appears to rely on *Lewis* for the proposition that Plaintiff did not have a right of privacy. In *Lewis*, the court held that use of a two-way mirror in a dressing room was not an invasion of privacy because customers do not have a legitimate expectation of privacy in light of signs posted in the dressing room indicating there was surveillance. It is not clear how this case is applicable to the instant facts, it is undisputed that Plaintiff was unaware of Defendant's use of the key logger.

Defendant also cites *Saldana v. Kelsey-Hayes Company*, 178 Mich.App. 230 (Mich.App. 1989), where the court found an employer's use of a high powered lens to look into an employee's home for purposes of determining whether he was disabled was not an invasion of privacy. The court found the plaintiff did not have a right to privacy because the surveillance

"involved matters which defendants had a legitimate right to investigate." *Id.* at 234. The court found that an employer has a legitimate right to investigate suspicions that an employee's work-related disability is a pretext. *Id.* at 235. This case is not dispositive of Plaintiff's claim.

Defendant asserts that he had a right to monitor Plaintiff's computer activities in the interests of himself, Plaintiff, and their children. [Motion, p.26]. However, Plaintiff presents evidence that Defendant continued to access her private email after the divorce, and regarding matters that were no longer of Defendant's concern. [Plaintiff's Exhibit A]. In general, Plaintiff had a right to privacy in her private email account.

Plaintiff raises an issue of fact regarding whether Defendant Bailey's use of a key logger to learn her email and messaging passwords so that he could access her private correspondence was objectionable to a reasonable man. See *Saldana*, 178 Mich.App. at 234 ("[w]hether the intrusion is objectionable to a reasonable person is a factual question best determined by a jury."). Defendant Bailey is not entitled to summary judgment on this claim.

**2. Public disclosure of private facts**

"A cause of action for public disclosure of embarrassing private facts requires (1) the disclosure of information, (2) that is highly offensive to a reasonable person, and (3) that is of no legitimate concern to the public." *Doe*, 212 Mich.App. at 80. Further, as the name of the claim implies, the information must be disclosed to the public. *Duran v. The Detroit News, Inc.*, 200 Mich.App. 622, 631 (Mich.App. 1993).

The alleged "public" disclosure of the information contained in Plaintiff's emails consists of Defendant Pope's use of the emails to impeach Plaintiff's testimony during a custody hearing, although he did not admit them into evidence; copies were sent as exhibits to Plaintiff's attorney,

Defendant Kozyra; and the emails were summarized in response to a motion by Plaintiff. None of these is sufficient to support Plaintiff's claim for invasion of privacy based on public disclosure of private facts.

The information disclosed, regarding Plaintiff's sexual relations, were private facts. "Sexual relations, for example, are normally entirely private matters." *Doe*, 212 Mich.App. at 82 (citation omitted). However, the information must be of no legitimate concern to the public. All of the disclosures were in the context of a court case to determine the custody of the parties three children. Where the state is required to determine the custody of children during a divorce, the fitness of a person to parent is of legitimate concern to the public. Thus, this was not "unreasonable publicity." See *Doe*, 212 Mich.App. at 81.

Accordingly, Defendants are entitled to summary judgment on this claim.

**G. Intentional Infliction of Emotional Distress**

Plaintiff alleges a claim of intentional infliction of emotional distress against all Defendants. In order to establish her claim, Plaintiff must prove: (1) extreme and outrageous conduct; (2) intent or recklessness; (3) causation; and (4) severe emotional distress. *Lewis*, 258 Mich.App. at 196. "Liability attaches only when a plaintiff can demonstrate that the defendant's conduct is 'so outrageous in character, and so extreme in degree, as to go beyond all possible bounds of decency, and to be regarded as atrocious and utterly intolerable in a civilized community.'" *Id.* (citation omitted). "The test to determine whether a person's conduct was extreme and outrageous is whether recitation of the facts of the case to an average member of the community 'would arouse his resentment against the actor, and lead him to exclaim, Outrageous!'" *Id.* (citation omitted).

In this case, Defendants' conduct of using a key logger to obtain Plaintiff's passwords in order to gain access to her email and messaging accounts, and then using copies of those documents in divorce and custody proceedings is not extreme and outrageous conduct. A husband snooping in his wife's email, after learning that she was engaging in sexual discussions over the internet while the children may have been present, and using damaging emails in divorce and custody proceedings can hardly be considered "atrocious and utterly intolerable in a civilized society." Consistent with the discussion above regarding Plaintiff's invasion of privacy claim, Defendant Bailey's method of garnering the information may be objectionable to a reasonable man, that is for the jury to decide, but his conduct does not "go beyond all possible bounds of decency."

Defendants are entitled to summary judgment on Plaintiff's claim for intentional infliction of emotional distress.

**H. Subject Matter Jurisdiction**

The only remaining claim against Defendant Kozyra, is for professional negligence based on his representation of Plaintiff in her state court proceedings. "[F]ederal courts have an independent obligation to investigate and police the boundaries of their own jurisdiction." *Douglas v. E.F. Baldwin & Associates, Inc*., 150 F.3d 604, 607 (6th Cir. 1998). Although Kozyra has not brought a motion before this Court, the Court may review the issue of subject matter jurisdiction sua sponte.

Plaintiff's claim arises under state law, thus the basis for subject matter jurisdiction is supplemental jurisdiction. 28 U.S.C. § 1367. Section 1367(a) provides that the court has supplemental jurisdiction "over all other claims that are so related to claims in the action within

such original jurisdiction that they form part of the same case or controversy." See United Mine Workers of America v. Gibbs, 383 U.S. 715, 725 (1966)(In order to exercise pendent jurisdiction, "[t]he state and federal claims must derive from a common nucleus of operative fact."). Plaintiff's professional negligence claim is not a part of the same "case or controversy" and does not arise from a "common nucleus of operative fact" as the claims pertaining to Defendants' access and use of Plaintiff's private emails.

Accordingly, this Court cannot exercise supplemental jurisdiction over Plaintiff's professional negligence claim. To the extent the Court could exercise jurisdiction over the claim, it declines to do so under 28 U.S.C. § 1367 (c). Therefore, because this was the only remaining claim against him, Defendant Andrew Kozyra is dismissed from this action.

## IV. CONCLUSION

For the foregoing reasons, the Court **GRANTS** Defendant Todd Pope's Motion for summary judgment; and **GRANTS** in part, and **DENIES** in part, Defendant Jeffrey Bailey's Motion for summary judgment. Summary judgment is granted on Plaintiff's claims for: (1) violation of 18 U.S.C. § 2511; (2) violation of 18 U.S.C. § 2512; (3) MCL § 750.539a, et seq.; (4) MCL § 750.540; (5) invasion of privacy against Defendant Pope based on intrusion upon seclusion; (6) invasion of privacy based on public disclosure; and (7) intentional infliction of emotional distress. Summary judgment is denied on Plaintiff's claims for: (1) violation of 18 U.S.C. § 2701 against Defendant Bailey; and (2) invasion of privacy against Defendant Bailey based on intrusion upon seclusion. Additionally, Defendant Andrew Kozyra is **DISMISSED**

from this action.

**IT IS SO ORDERED.**

Dated: February 6, 2008

s/ Sean F. Cox
U. S. District Court Judge

---

**PROOF OF SERVICE**

The undersigned certifies that the foregoing order was served upon counsel of record via the Court's ECF System and/or U. S. Mail on February 6, 2008.

s/Jennifer Hernandez
Case Manager to
District Judge Sean F. Cox